TLP:WHITE

SICK PSIRT
Security Advisory

Inadequate SSH configuration in Visionary-S CX

Document ID:	SCA-2021-0001
Publication Date:	2021-06-25
CVSSv3 Base Score:	3.7 (CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:L/I:L/A:N)
CVE Identifier:	CVE-2021-32496
CWE Identifier:	CWE-326
Version:	V1.0

SUMMARY

SICK received a report that informed SICK about an Inadequate Encryption Strength vulnerability in the SICK product "Visionary-S CX" concerning the internal SSH interface solely used by SICK for recovering returned devices.
The use of weak algorithms makes it easier for an attacker to break the security that protects information transmitted from the client to the SSH server, assuming the attacker has access to the network on which the device is connected. This can increase the risk that encryption will be compromised, leading to the exposure of sensitive user information and man-in-the-middle attacks.
SICK has developed a hotfix. In released firmware versions greater than 5.21.2.29154 the SSH server will no longer offer these weak ciphers.
Currently SICK is not aware of any public exploits specifically targeting this vulnerability.

AFFECTED PRODUCTS

Product	Version	Remediation available
Visionary-S CX	All versions < 5.21.2.29154R	Yes (Hotfix upon customer request)

The vulnerability is not visible in any supported customer functionality. Thus customers can only identify products by firmware version. Accessing the device via SSH now shows OpenSSH instead of dropbear.

General Security Practices

As general security measures, SICK recommends to minimize network exposure of the devices, restrict network access and follow recommended security practices in order to run the devices in a protected IT environment.
Additional information on Industrial Security can be found at:
http://ics-cert.us-cert.gov/content/recommended-practices

VULNERABILITY CLASSIFICATION

SICK performs vulnerability classification by using the CVSS scoring system (CVSS v3.x). The environmental score is dependent on the customer's environment and can affect the overall CVSS

score. SICK recommends that customers individually evaluate the environmental score to achieve final scoring.

From the BSI there is the following Technical Guideline for the use of the cryptographic protocol Secure Shell (SSH).
https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-4.pdf

RESOURCES

CVSS Calculator
https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

SICK PSIRT Security Advisories
https://sick.com/psirt

ICS-CERT recommended practices on Industrial Security
http://ics-cert.us-cert.gov/content/recommended-practices

BSI Technical Guidance
https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-4.pdf

HISTORY

Version	Release Date	Comment
V1	2021-06-25	Initial Release